ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Факультет компьютерных наук
Образовательная программа бакалавриата «Программная инженерия»

СОГЛАСОВАНО Научный руководитель, профессор департамента программной инженерии факультета компьютерных наук канд. техн. наук	УТВЕРЖДАЮ Академический руководитель образовательной программы «Программная инженерия» профессор департамента программной инженерии, канд. техн. наук
_____ С.М. Авдошин «___» _____ 2020 г.	_____ В.В. Шилов «___» _____ 2020 г.

Подп. и дата	
Инв. № дубл.	
Взам. инв. №	
Подп. и дата	
Инв. № подл	

ПРОГРАММА КЛАССИФИКАЦИИ КОМПЬЮТЕРНЫХ АТАК ПО НАБОРУ ДАННЫХ ISCX BOTNET

Руководство оператора

ЛИСТ УТВЕРЖДЕНИЯ

RU.17701729.02.13-01 34 01-1-ЛУ

Исполнитель
студент группы БПИ193
_____ /Е.А. Гриценко /
«____»_____ 2020 г.

Москва 2020

УТВЕРЖДЕН
RU.17701729.02.13 -01 34 01-1-ЛУ

Подп. и дата	
Инв. № дубл.	
Взам. инв. №	
Подп. и дата	
Инв. № подл	

ПРОГРАММА КЛАССИФИКАЦИИ КОМПЬЮТЕРНЫХ АТАК ПО НАБОРУ ДАННЫХ ISCX BOTNET

Руководство оператора

RU.17701729.02.13-01 34 01-1

Листов 16

Москва 2020

ОГЛАВЛЕНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

Программа предназначена для классифкации сетевых потоков в файле с информацией о них, трафике с доступных сетевых устройств или его дампе как порождённых ботнетом или же обычных потоков, с возможностью дополнения и использования с иными пользовательскими классификаторам, в частности, небинарными без рекомпиляции (plug-in). Также программа предназначена для установления точности классификаторов путём их выполнения на файлах, содержащих информацию о потоках и метках к ним. Программа обладает консольным интерфейсом.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1. Зависимости

Программа использует .NET Framework 4.7. Соответственно, необходимо, чтобы был корректно установлен и работоспособен либо он, либо совместимые реализации (например, Mono).

Также программа использует следующие библиотеки .NET, поставляемые вместе с ней: SharpPcap 5.1.0, PacketDotNet 1.0.3, System.Runtime.CompilerServicies.Unsafe 4.6.0. Должна быть обеспечена их корректная работа, для этого, как минимум, необходимо наличие их зависимостей. SharpPcap использует libpcap на ОС, основанных на GNU/Linux, и npcap на ОС семейства Windows. Соответственно, для корректной работы SharpPcap на описанных системах необходимы наличие и работоспособность этих библиотек.

2.2. Загрузка библиотек, поставляемых вместе с приложением

Для запуска приложения необходимо, чтобы реализациям .NET были доступны все файлы библиотек-зависимости, поставляемые вместе с приложением. Таковыми из поставляемых являются файлы с расширением “dll”.

2.3. Разрешения

У пользователя, от имени которого запускается приложение, должны быть разрешение на чтение библиотек-зависимостей, поставляемых вместе с ПО и разрешение на выполнение программы. Для прослушивания трафика живых устройств и получения их списка, чтения файлов по передаваемым путям и их записи, у пользователя также должны быть соотвтветствующие разрешения. Таковыми же разрешениями должно обладать и само приложение, если наличествует контроль доступа для отдельных программ.

2.4. Вычислительная мощность и память

Для проведения анализа сетевых потоков в реальном времени необходимо, что ОС выделяла программе вычислительные мощности соответствующие скорости трафика и числу соединений. Для обработки сетевых потоков с живых устройств и PCAP-файлов необходимо наличие памяти соответствующее количеству соединений; нарушение этого требования может повлечь за собою аварийное завершение приложения системой или

сбой ОС. ОС должна быть способна предоставить приложению как минимум 256 MiB оперативной памяти.

2.5. Отсутствие сбоев

Необходимо отсутствие влияния других программ на оперативную память данного приложения, сбоев ОС, сбоев электропитания, механических и иных повреждений ЭВМ, на которой запущено или планируется запускать приложение.

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1. Установка ПО

Если зависимости ПО, описанные в главе 2.1 не установлены, то таковая установка должна быть произведена. Так для ОС, основанных на GNU/Linux, рекомендуется установка mono и libpcap, на Windows — .NET Framework 4.7 и npcap.

В случае, если установка производится на ОС, основанной на GNU/Linux, предлагаются два следующих варианта установки.

Первый. Библиотеки-зависимости из архива с ПО либо копируются в директорию, из которой используемая для запуска реализация .NET (далее: реализация .NET) осуществляет загрузку библиотек (таковой директорией может быть /lib для mono), либо копируются в директорию, которую необходимо указать как директорию для загрузки библиотек реализацией .NET. Файл BotnetDetector.exe и скрипт botnetdetector копируются в папку, прописанную в системной переменной PATH (например /bin), в скрипте строка /opt/BotnetDetector/BotnetDetector.exe заменяется на путь к BotnetDetector.exe, корректно обрабатываемый командной оболочкой (например, заключённый в кавычки, если он содержит пробелы). Если была использована иная реализация .NET, нежели mono, то необходимо заменить команду запуска в скрипте на верную согласно документации этой реализации. Далее для пользователей, от имени которых планируется запуск программы, следует при необходимости установить разрешения согласно главе 2.3.

Второй. В /opt (или иной директории) создаётся папка BotnetDetector (или иная), в неё из архива копируются библиотеки-зависимости и файл BotnetDetector.exe. Если путь к выбранной папке не является путём для загрузки библиотек реализацией .NET, то его необходимо добавить как таковой. Далее скрипт botnetdetector копируются в папку, прописанную в системной переменной PATH (например /bin). Если путь к BotnetDetector.exe отличен от прописанного в скрипте, то его необходимо изменить на верный, корректно обрабатываемый командной оболочкой (например, заключённый в кавычки, если он содержит пробелы). Если была использована иная реализация .NET, нежели mono, то необходимо заменить команду запуска в скрипте на верную согласно документации этой реализации. Далее для пользователей, от имени которых планируется запуск программы, при необходимости установить разрешения согласно главе 2.3.

В случае же, если установка производится на ОС Windows, то предлагаемый способ подразумевает использование .NET Framework 4.7. Из архива в выбранную для установки папку копируются библиотеки-зависимости и файл BotnetDetector.exe. После чего путь к папке прописывается в переменную PATH, используемую системой для пользователей, от имени которых планируется запускать приложение. Далее для пользователей, от имени которых планируется запуск программы, при необходимости установить разрешения согласно главе 2.3.

3.2. Корректная комманда запуска

В случае, если был выбран один из предложенных вариантов установки на ОС, основанную на GNU/Linux, корректая команда запуска — “botnetdetector” (имя скрипта, передающего параметры настоящей программе). В случае, если был выбран предложенный вариант установки на Windows, то корректная команда запуска — “BotnetDetector”.

3.3. Интерфейс программы

Выполнение программы может осуществляться посредством терминала или скрипта (для подавления консольного вывода о статусе можно воспользоваться опцией “-q”). Управление параметрами запуска программы осуществляется через её аргументы. Передача аргументов программы осуществляется способом, специфичным для коммандной оболочки, в которой запускается программа. Аргументы подразделяются на два типа: опции и аргументы этих опций. Аргументы для каждой опции должны указываться следующими аргументами после каждой опции, согласно нижеизложенному описанию для каждой. Опции могут переопределять ранее указанное предыдушими опциями поведение программы. Порядок не влияющих и не переопределяющих друг друга опций может быть любым. Далее

- Опциями-флагами называются опции “--absoluteClassifierPath”, “--classifiy”, “--printFlows”, “--printClasses”, “--printAbnormalOnly”, “--nameAbnormalAsBotnet”, “--skipFirstLine”. Каждая из этих опций определяет поведение, которое может быть либо включено, либо выключено. Если для опции-флага не указано одним из следующих аргументов её состояние, посредством опций “-0” (выключить) и “-1” (включить), то считается, что поведение, определённое этой опцией-флагом включается.

- Опциями, определяющими работу программы являются опции “-l”, “--live”, “-p”, “--pcap”, “-t”, “--table”, “-h”, “--help”, “-pr”, “--performance”, “-ls”, “--listDevicies”. Эти опции непосредственно определяют задачу, выполняемую программой. Выполняется работа, определяемая последней указанной такой опцией (они переопределяют друг друга). Если ни одна из таких опций не указана, то печатается сообщение помощи, являющееся кратким описанием опций. При этом опциями, задающими работу программы с сетевыми потоками (их захват и классификацию), являются “-l”, “--live”, “-p”, “--pcap”, “-t”, “--table”. Полный перечень опций с их описанием:

3.3.1. “-h”, “--help” указывают программе, что она должна напечатать в стандартный вывод сообщение помощи с кратким описанием опций.

3.3.2. “-l”, “--live” указывают программе, что она должна прослушивать трафик с устройства, и выводить информацию о сетевых потоках и их классах. Устройство задаётся по имени через аргумент опции ввода “-i”, “--input”. Если таковых несколько, то используется последний. Имена доступных устройств можно посмотреть воспользовавшись опцией “-ls” или “--listDevicies”. Файл, в который осуществляется вывод задаётся с помощью опции “-o” или “--output”. Если он не был предоставлен, печать осуществляется в стандартный вывод. Прервать выполнение программы можно нажатием сочетания клавиш отмены (Ctrl+C для Linux).

3.3.3. “-p”, “--pcap” указывает программе, что она должна читать PCAP-файл, и выводить информацию о сетевых потоках и их классах. Файл задаётся по имени через аргумент опции ввода “-i”, “--input”. Если таковых несколько, то используется последний. Файл, в который осуществляется вывод задаётся с помощью опции “-o” или “--output”. Если он не был предоставлен, печать осуществляется в стандартный вывод.

3.3.4. “-t”, “--table” указывает программе, что она должна читать CSV-подобный файл с информацией о сетевых потоках, и выводить информацию о них и их классах. Файл задаётся по имени через аргумент опции ввода “-i”, “--input”. Если таковых несколько, то используется последний. Если первая строка в файле не является информацией о потоке, то для чтения такого файла необходимо указать опцию “--skipFirstLine”. Файл, в который осуществляется вывод задаётся с помощью опции “-o” или “--output”. Если он не был предоставлен, печать осуществляется в стандартный вывод.

3.3.5. “-pr”, “--performance” указывает программе, что она должна вычислить точность классификатора, используя указанный CSV-подобный файл с информацией о потоках и их классах. Файл задаётся по имени через аргумент опции ввода “-i”, “--input”. Если таковых несколько, то используется последний. Если первая строка в файле не является информацией о потоке, то для чтения такого файла необходимо указать опцию “--skipFirstLine”. Печать статистики всегда осуществляется в стандартный вывод.

3.3.6. “-ls”, “--listDevicies” указывает программе, что она должна вывести в стандартный вывод устройства, доступные для прослушивания.

3.3.7. “-i”, “--input” используются для указания пути файла или имени устройства как источника данных для выполнения работы. У опции один обязательный аргумент — путь файла или имя устройства. Имена доступных устройств можно посмотреть воспользовавшись опцией “-ls” или “--listDevicies”.

3.3.8. “-o”, “--output” используется для указния пути файла, в который должен производиться вывод. Аргумент опции — путь к файлу. Файл будет перезаписан, если существует. Опция не влияет на “-ls” (“--listDevicies”), “-h” (“--help”), “-pr” (“--performance”): если работа задана этими опциями, то печать всегда осуществляется в стандартный вывод.

3.3.9. “--classifier” используется для указания библиотеки-классификатора, с помощью которой производить классифицацию. Первым аргументом указывается путь к библиотеке, вторым полное имя типа класса классификатора, который необходимо загузить. При этом по умолчанию путь классификатора считается относительным, изменить это можно использованием опции-флага “--absoluteClassifierPath”. Программе можно указать использовать стандартный классификатор, в таком случае единственным аргументом опции должна быть строка “-0”. Вадидный классификатор должен быть публичным, и унаследованным от класса AbstractClassifier библиотки LibBtntDtct, иметь публичный конструктор без параметров и корректно реализовывать все абстрактные члены базового класса. Более подробная информациия о том, каким должен быть валидный классификатор находится в руководстве программиста [3].

3.3.10. “--classify” опция-флаг, используется для указания, классифицировать сетевые потоки или нет. Включена по умолчанию. Опция влияет только на “-l” (“--live”), “-p” (“--pcap)”, “-t” (“--table”). Если эта опция отключена, то классификация и, соответственно,

печать имён классов и печать статистики о классах не производятся, помимо этого всегда происходит печать для всех сетевых потоков. Выключить опцию можно добавив следующим аргументов опцию “-0”.

3.3.11. “--printFlows” опция-флаг, используется для указания, печатать информацию о потоках или нет. Включена по умолчанию. Опция влияет только на “-l” (“--live”), “-p” (“--pcap)”, “-t” (“--table”). Если эта опция отключена, то печать информации о сетевых потоках не производится. Выключить опцию можно добавив следующим аргументов опцию “-0”.

3.3.12. “--printClasses” опция-флаг, используется для указания, печатать информацию о классах потоков или нет. Включена по умолчанию. Опция влияет только на “-l” (“--live”), “-p” (“--pcap)”, “-t” (“--table”). Если эта опция отключена, то печать имён классов сетевых потоков не производится. Выключить опцию можно добавив следующим аргументов опцию “-0”.

3.3.13. “--printAbnormalOnly” опция-флаг, отключенная по умолчанию. Если включена, то производится печать только для тех сетевых потоков, имя класса которых не равно “normal”. Опция влияет только на “-l” (“--live”), “-p” (“--pcap)”, “-t” (“--table”). Не имеет эффекта, если классификация отключена. Включение и отключение классификации определяется опцией “--classify”.

3.3.14. “--nameAbnormalAsBotnet” опция-флаг, отключенная по умолчанию. Если включена, то все классы, имя которых не равно “normal”, объеденяются в общий надкласс “botnet”. Таким образом, при печати статистики и имён классов, будут использоваться только два класса: “normal” и “botnet”. Опция влияет только на “-l” (“--live”), “-p” (“--pcap)”, “-t” (“--table”). Не имеет эффекта, если классификация отключена. Включение и отключение классификации определяется опцией “--classify”.

3.3.15. “--skipFirstLine” опция-флаг, отключенная по умолчанию. Влияет только на “-t” (“--table”) и “-pr” (“--performance”). Если включена, то при чтении CSV-подобного файла первая строка пропускается, и парсинг информации начинается со второй строки.

3.3.16. “-0” опция, выключающая последнюю переданную опцию-флаг.

3.3.17. “-1” опция, включающая последнюю переданную опцию-флаг.

3.3.18. “-v”, “--verbose” указывает программе печатать больше внутренней информации, которая может быть полезна для отладки. В текущей версии позволяет печатать полный стэк исключений в случае ошибок чтения аргументов, чтения файлов и так далее.

3.3.19. “-q”, “--quiet” указывает программе не производить печать статуса работы в консольный вывод. Может использоваться для «тихой» работы: демонизации программы и её использования в скриптах.

3.4. Указания по работе с входными и выходными данными

Результатами работы программы, в случае, когда посредством неё производится класификация сетевых потоков и запись их и имён их классов в файл, является CSV (comma separated values) файл. Каждая строка таблицы является либо строкой информации о потоке (файл с информацией о потоках), либо именем класса (файл с информацией о классах), либо строкой, где сначала идут ячейки информации о потоке, затем ячейка имени класса (файл с информацией о классированных потоках) — в зависимости от аргументов программы. Строка с информацией о потоке включает (по порядку): время первого пакета, время последнего пакета, IP-адрес отправителя, порт отправителя (0, если не TCP или UDP), IP-адрес получателя, порт получателя (0, если не TCP или UDP), номер протокола, число пакетов, число исходящих пакетов, число октет, число октет в payloade (подробное описание их расчёта находится в пояснительной записке [2]).

Подаваемые на вход файлы имеют CSV-подобный формат, каждая строка таблицы является либо строкой информации о потоке (файл с информацией о потоках), либо строкой, где сначала идут ячейки информации о потоке, затем ячейка имени класса (файл с информацией о классированных потоках). Следует отметить, что файлы, подаваемые на вход, не поддерживают CSV-формат в полной мере, а именно — не поддерживают кавычки как символы-ограничители значения ячейки. Поэтому при подготовке входных данных для приложения необходимо учесть это обстоятельство. Также следует учесть то обстоятельство, что при чтении имени класса потока, крайние левые и правые пробелы удаляются, поэтому их использование в имени не разрешено.

Форматы выходных данных при классификации, если производится вывод информаций о потоках и их классах, совместим с форматом входных. Таким образом, программа может быть использована сначала — для захвата информации о потоках из

живого трафика или дампа, а уже потом — для классификации ранее захваченной информации о потоках.

Под CSV-файлом понимается файл таблицы, значения которого разделены именно запятыми, а не ‘;’, поэтому Excel на Windows с русскоязычной локализацией по умолчанию не сможет отобразить в виде таблицы оговариваемый вывод программы: Excel не поддерживает параметризацию символов-делиметров списка, и использует значение символа-делиметра, определяемого локалью. Поэтому для открытия производимых программой файлов Excel-ом в Windows возможна необходимость изменения параметров локали. Вследствие чего, для представления этих файлов в наглядной табличной форме рекомендуется воспользоваться LibreOffice Calc.

Полная спецификация форматов данных описана в ТЗ в главе 4.1.2.

4. СООБЩЕНИЯ ОПЕРАТОРУ

Ниже приведены примеры некоторых сообщений оператору.

Сообщение помощи, выводящееся в случае, если выбран показ помощи или не были выбраны опции.

```
[someuser@somehost BotnetDetector]# mono BotnetDetector.exe
Use:
-h, --help                                  to print this message.
-l, --live                                  to process live device packets.
-p, --pcap                                  to process pcap file.
-t, --table                                 to process flows from a table given.
-pr, --performance                          to evaluate performance on a labeled flow table.
-ls, --listDevicies                         to list devicies available for live capture.
-i, --input                                 to specify input parameters like file or device name.
-o, --output                                to specify output parameters like file name. If no file provided stdout is used.
--classifier pathToAssembly fullTypeName    to use a classifier in the assembly.
--absoluteClassifierPath                    to consider path to classifier assembly to be absolute.
--classify                                  to specify that trafic should be clasified. Enabled by default.
--printFlows                                to specify that flows should be printed. Enabled by default.
--printClasses                              to specify that flows should be printed. Enabled by default.
--printAbnormalOnly                         to specify that only abnormal trafic should be printed.
--nameAbnormalAsBotnet                      to name trafic classified as not normal as botnet.
--skipFirstLine                             to skip first line when reading a flow table file.
-0                                          to disable a bool option or restore some to default.
-1                                          to enable a bool option.
-v, --verbose                               to be verbose. This includes showing full error trace.
-q, --quiet                                 to supress all state noticies to stdout except errors.
[someuser@somehost BotnetDetector]# _
```

Сообщение, выводящееся оператору в случае, если самая правая опция требует больше аргументов: “More arguments expected for the rightmost option”.

Пример сообщения, выводящеегося оператору в случае, если выбранная обция не распознана.

```
[someuser@somehost BotnetDetector]# mono BotnetDetector.exe --live --gimmeWhatIWant -i wlo
Unrecognised option --gimmeWhatIWant
```

Пример статистики прочитанных пакетов и распознанных потоков при захвате с живого устройства.

```
Packets statistics:
Total: 75373
Queued: 0 / 1000000 (max)
Errors: 0
Droped: 0
Flows statistics:
74      normal
52      botnet
[someuser@somehost BotnetDetector]# _
```

Пример вывода информации о классированных потоках в консоль. При выводе в файл используется тот же формат.

```
10.08.2011 09:19:41.705073, 10.08.2011 09:19:50.721416,147.32.84.165, 1666, 222.88.205.195, 443, 6,6, 6, 288, 0, botnet
10.08.2011 09:19:41.705182, 10.08.2011 09:19:50.721539,147.32.84.165, 1650, 85.13.145.7, 25, 6,6, 6, 288, 0, botnet
10.08.2011 09:19:41.904924, 10.08.2011 09:19:50.918023,147.32.84.165, 1651, 65.54.188.110, 25, 6,6, 6, 288, 0, botnet
10.08.2011 09:19:43.007116, 10.08.2011 09:19:46.010855,147.32.84.165, 1670, 83.229.32.202, 6667, 6,4, 4, 192, 0, botnet
10.08.2011 09:19:43.007255, 10.08.2011 09:19:52.019489,147.32.84.165, 1652, 64.12.90.33, 25, 6,6, 6, 288, 0, botnet
10.08.2011 09:19:43.591055, 10.08.2011 09:20:05.362104,212.117.171.138, 65500, 147.32.84.165, 1643, 6,17, 5, 736, 56, botnet
10.08.2011 09:19:43.707525, 10.08.2011 09:19:52.720715,147.32.84.165, 1653, 74.125.113.27, 25, 6,6, 6, 288, 0, botnet
10.08.2011 09:19:43.907809, 10.08.2011 09:19:43.907815,147.32.84.165, 1630, 222.88.205.195, 443, 6,2, 2, 328, 248, botnet
10.08.2011 09:19:44.007999, 10.08.2011 09:20:06.835173,147.32.84.165, 1672, 212.117.171.138, 65500, 6,66, 42, 5892, 3228, botnet
10.08.2011 09:19:44.008131, 10.08.2011 09:19:53.021050,147.32.84.165, 1654, 209.191.88.254, 25, 6,6, 6, 288, 0, botnet
10.08.2011 09:19:44.308505, 10.08.2011 09:19:53.321577,147.32.84.165, 1673, 209.191.88.254, 25, 6,6, 6, 288, 0, botnet
10.08.2011 09:19:44.308637, 10.08.2011 09:19:53.321712,147.32.84.165, 1656, 66.94.238.147, 25, 6,6, 6, 288, 0, botnet
10.08.2011 09:19:49.989022, 10.08.2011 09:19:49.989031,147.32.84.165, 1293, 95.211.58.97, 8399, 17,2, 2, 58, 2, botnet
10.08.2011 09:19:50.781440, 10.08.2011 09:19:50.781713,147.32.96.45, 2051, 147.32.84.165, 21, 6,3, 1, 140, 0, botnet
10.08.2011 09:19:51.518838, 10.08.2011 09:20:00.531738,147.32.84.165, 1657, 205.188.59.193, 25, 6,6, 6, 288, 0, botnet
10.08.2011 09:19:51.518971, 10.08.2011 09:20:00.531865,147.32.84.165, 1659, 66.94.238.147, 25, 6,6, 6, 288, 0, botnet
10.08.2011 09:19:51.519025, 10.08.2011 09:20:00.531919,147.32.84.165, 1661, 64.12.90.33, 25, 6,6, 6, 288, 0, botnet
10.08.2011 09:19:51.519081, 10.08.2011 09:20:00.531969,147.32.84.165, 1662, 194.177.250.245, 25, 6,6, 6, 288, 0, botnet
10.08.2011 09:19:55.224897, 10.08.2011 09:19:58.228368,147.32.84.165, 1680, 62.209.146.67, 6667, 6,4, 4, 192, 0, botnet
10.08.2011 09:19:55.225013, 10.08.2011 09:20:04.236875,147.32.84.165, 1664, 66.94.238.147, 25, 6,6, 6, 288, 0, botnet
10.08.2011 09:19:55.225046, 10.08.2011 09:19:55.510466,147.32.84.165, 1665, 213.246.53.125, 5296, 6,11, 8, 464, 0, botnet
10.08.2011 09:19:55.323407, 10.08.2011 09:20:04.237000,147.32.84.165, 1667, 74.125.67.27, 25, 6,6, 6, 288, 0, botnet
10.08.2011 09:20:01.733579, 10.08.2011 09:20:10.646172,147.32.84.165, 1687, 173.192.170.88, 80, 6,6, 6, 288, 0, botnet
10.08.2011 09:20:02.735215, 10.08.2011 09:20:11.647707,147.32.84.165, 1668, 216.32.181.178, 25, 6,6, 6, 288, 0, botnet
10.08.2011 09:20:02.935402, 10.08.2011 09:20:02.957876,147.32.84.165, 1685, 212.117.171.138, 65500, 6,5, 4, 224, 0, botnet
10.08.2011 09:20:02.935500, 10.08.2011 09:20:11.847931,147.32.84.165, 1669, 66.94.238.147, 25, 6,6, 6, 288, 0, botnet
10.08.2011 09:20:02.935529, 10.08.2011 09:20:06.940977,147.32.84.165, 1689, 64.12.168.40, 587, 6,41, 26, 4725, 3061, normal
```

Пример результата вычисления точности классификатора.

```
289893 flows have been processed.
Processed 290574 flows.
Computed: 208572 (71.779%) as normal,   82002 (28.221%) as botnet.
Real: 197854 (68.091%) as normal,       92720 (31.909%) as botnet.

Botnet/normal classes validation results:
79490 (27.356%) TP,     195342 (67.226%) TN,    274832 (94.582%) True
2512 (0.864%) FP,       13230 (4.553%) FN,      15742 (5.418%) False

Flows contributed to FN were follows:
neris: 1049 (7.929%)
rbot: 664 (5.019%)
virut: 150 (1.134%)
nsis: 1553 (11.738%)
smtp_spam_storm: 9793 (74.021%)
smtp_spam_waledac: 1 (0.008%)
zeus_cc: 12 (0.091%)
zeus: 8 (0.060%)

By class comparision:
neris: 16999 (5.850%) computed, 24548 (8.448%) real
rbot: 50546 (17.395%) computed, 40848 (14.058%) real
virut: 290 (0.100%) computed,   987 (0.340%) real
nsis: 6305 (2.170%) computed,   8742 (3.009%) real
smtp_spam_storm: 7858 (2.704%) computed,        17570 (6.047%) real
normal: 208572 (71.779%) computed,      197854 (68.091%) real
smtp_spam_waledac: 0 (0.000%) computed, 1 (0.000%) real
zeus_cc: 2 (0.001%) computed,   14 (0.005%) real
zeus: 2 (0.001%) computed,      10 (0.003%) real
[someuser@somehost BotnetDetector]# _
```

5. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. «Программа классификации компьютерных атак по набору данных ISCX Botnet».

Техническое задание;

2. «Программа классификации компьютерных атак по набору данных ISCX Botnet».

Пояснительная записка;

3. «Программа классификации компьютерных атак по набору данных ISCX Botnet».

Руководство программиста.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	№ документа	Входящий № сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					